CLAIMS

What is claimed is:

1. A machine readable media, comprising:

a writeable area of the media;

a read only area of the media;

a content stored on the writeable area of the media;

a first media validation data containing an encrypted preselected value and being stored on the writeable area; and,

a second media validation data equal to the first media validation data and being stored on the read only area.

2. The media of claim 1, further comprising:

a circuit to calculate a message authentication code over the first media validation data using a shared session key to be established between the media and a device authorized to access the content.

3. The media of claim 1 is a digital versatile disc (DVD).

4. A device comprising:

an input/output apparatus to access a media; and,

a processor communicatively coupled with the input/output apparatus, the processor being configured to

read a first media validation data from a writeable area of the media,

set a first device validation data equal to the first media validation data,

read a second media validation data from a read only area of the media,

set a second device validation data equal to the second media validation data,

compare the first device validation data and the second device validation data, and

deny authorization to access content stored on the media if the first device validation data and the second device validation data are unequal.

5. The device of claim 4, wherein the processor is further configured to decrypt one of the first device validation data and the second device validation data and to deny authorization to access the content if a result of the decryption is unequal to a preselected value.

6. The device of claim 4, wherein the processor is further configured to:

establish a shared session key with the media,

read a first media message authentication code from the media,

set a first device message authentication code equal to the first media message authentication code,

calculate a second device message authentication code over the first media validation data using the shared session key,

compare the first device message authentication code and the second device message authentication code, and

deny authorization to access a content stored on the media if the first device message authentication code and the second device message authentication code are unequal.

7. The device of claim 4 is a digital versatile disc (DVD) player.

8. A data protection system, comprising:

a media including (i) a writeable area that stores a first media validation data containing an encrypted preselected value and a content, (ii) a read only area of the media that stores a second media validation data equal to the first media validation data.

a processor communicatively coupled with the media, the processor being configured to read the first media validation data, set a first device validation data equal to the first media validation data, read the second media validation data, set a second device validation data equal to the second media validation data, compare the first device validation data and the second device validation data, and deny authorization to access the content if the first device validation data and the second device validation data are unequal.

9. The data protection system of claim 8, further comprising:

a media circuit to calculate a media message authentication code over the second media validation data using a shared session key to be established when the processor attempts to access the content.

10. The data protection system of claim 8, wherein the processor is further configured to

establish the shared session key with the media,

read the media message authentication code from the media,

set a first device message authentication code equal to the media message authentication code,

calculate a second device message authentication code over the first device validation data using the shared session key,

compare the first and the second device message authentication codes and

deny authorization to access the content if the first and the second device message authentication codes are unequal.

11. The data protection system of claim 8, wherein the reader is a digital versatile disc (DVD) player.

12. A method, comprising:

preselecting a value;

encrypting the preselected value;

setting a first media validation data equal to the encrypted preselected value;

setting a second media validation data equal to the encrytpted preselected value;

storing the first media validation data on a writeable area of a media; and,

storing the second media validation data on a read only area of the media to protect a content stored on the media.

13. The method of claim 12, further comprising:

configuring a media processor to calculate a media message authentication code over the first media validation data using a shared session key to be established when a media reader attempts to access the content.

14. The method of claim 12, further comprising:

configuring a media reader to read the first media validation data;

setting a first device validation data equal to the first media validation data;

configuring the media reader to read the second media validation data;

setting a second device validation data equal to the second media validation data;

configuring the media reader to compare the first device validation data and the second device validation data; and,

configuring the media reader to deny authorization to access the content if the first device validation data and the second device validation data are unequal.

15. The method of claim 14, further comprising:

configuring the media reader to decrypt both the first device validation data and the second device validation data; and,

configuring the media reader to deny authorization to access the content if a result of the decryption is unequal to the preselected value.

16. The method of claim 12, wherein the media is a digital versatile disc (DVD).

17. A machine readable medium containing instructions which, when executed by an apparatus causes the apparatus to perform operations, comprising:

setting a first validation data equal to an encrypted preselected value;

setting a second validation data equal to the encrypted preselected value;

storing the first validation data on a writeable area of a media; and,

storing the second validation data on a read only area of the media.

18. The machine readable medium of claim 17, wherein the instructions, when executed, further cause the apparatus to perform operations comprising:

configuring a media processor to calculate a media message authentication code over the first media validation data using a shared session key to be established when a media reader attempts to access the content.

19. The machine readable medium of claim 17 is a digital versatile disc (DVD).

20. A machine readable medium containing instructions which, when executed by an apparatus, causes the apparatus to perform operations comprising:

configuring a media reader to read a first media validation data;

setting a first device validation data equal to the first media validation data;

configuring the media reader to read a second media validation data;

setting a second device validation data equal to the second media validation data;

configuring the media reader to compare the first device validation data and the second device validation data; and,

configuring the media reader to deny authorization to access the content if the first device validation data and the second device validation data are unequal.

21. The machine readable medium of claim 20, wherein the instructions, when executed further cause the apparatus to perform operations comprising:

configuring the media reader to decrypt both the first device validation data and the second device validation data; and,

configuring the media reader to deny authorization to access the content if a result of the decryption is unequal to the preselected value.

22. The machine readable medium of claim 20, the media reader is a digital versatile disk (DVD) player.

23. A machine readable media, comprising:

a writeable area of the media;

a read only area of the media;

a content stored on the writeable area of the media; and,

a first media validation data containing an encrypted preselected value and being stored on the read only area.

24. The machine readable media of claim 23, further comprising:

a second media validation data equal to the first media validation data and being stored on the writeable area.

25. The media of claim 23, further comprising:

a circuit to calculate a media message authentication code over the first media validation data using a shared session key to be established between the media and a device authorized to access the content.